Axcient

AIRGAP

Technology Overview

What is AirGap?

AirGap is part of Axcient's layered security approach that includes MFA, strong password policies, firewalls, spam filtering, phishing detection, and data redundancy. This is the last line of defense against ransomware attacks and human error. AirGap is enabled-by-default for all Axcient partners as part of the Replibit solution..

- Never even consider paying the ransom.
- Ensure that only legitimate deletion requests and backup data alterations are completed.
- Recover maliciously deleted backups after the attack has taken place.

How does AirGap work?

AirGap technology separates backup requests from the actual backup mechanics to prevent malicious deletion using the following unique features.

- "Honeypots" give bad actors the illusion they've accomplished their malicious goal – so they stop pursing corruption – but, in reality, the data is stored on isolated tiers of storage.
- Human factor controls limit authorized individuals who can create a deletion requests within the Axcient organization. This is separated from authorized individuals who can actually fulfill the deletion requests.
- Human two-factor authorization is required to verify the deletion request made using audible confirmation that the deletion request is valid. Even if the deletion request is malicious, in the event that phone, email and support systems are compromised, the request won't be processed without audible approval.
- Time gaps between when deletion requests are created, verified and executed give partners time to see and stop any malicious activity. The amount of time between processes vary so that patterns cannot be recognized and replicated.

Why is AirGap the best?

Competitors claim they protect against ransomware, but Axcient goes the extra step…

- AirGap was created after surveying the marketplace and first including what everyone else was offering as our "table stakes" – the elements of protection necessary just to be considered.
- Axcient researched advanced hacker behaviors to create security layers beyond MFA.
  - Today's hackers sit silently in systems for long periods of time while slowly reducing retention periods to minimize the amount of data being backed up.
  - Another common practice is to implement keylogging to discover duplicated admin passwords (a frowned upon, but common practice among techs).

- Axcient contracted two different security companies to complete independent testing. It’s not Axcient telling MSPs we’re secure, it’s verified by independent results
    - Tested the application, appliance and data center, along with phishing and social engineering attacks against data stored in Axcient’s datacenter.

Has AirGap been used in real life yet?

Yes. Although we just started informing the public about AirGap in early 2020, we launched it in its initial form in Q4 of 2019. Since then we’ve had some partners who were attacked multiple times by bad actors who were hiding in their systems for long periods of time.

Due to the hacker’s ability to sit on the network unnoticed for multiple days, they were able to obtain credentials for the local and offsite appliances. Before encrypting the production servers, they were able to delete local and offsite backups.

With what could have been a business ending attack. Axcient was able to do a quick restore with no ransom payment ever being considered.